УДК 004.56.5
ББК 32.972.53

Тугуз Н. С., Казачко А. А.
ФГБОУ ВО «Кубанский государственный аграрный университет имени И.Т. Трубилина» Краснодар, Россия

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И СПОСОБЫ ПОЛУЧЕНИЯ ЛИЧНЫХ ДАННЫХ МОШЕННИКАМИ

Аннотация: В данной статье рассматриваются способы кражи личных данных мошенниками и способы их предотвращение. В настоящее время стоит проблема конфиденциальности. Люди тщательно скрывают свои личные данные и доверяют их только проверенным сервисам, но недостаточно грамотные пользователи в IT сфере могут даже не подозревать о том, что они в, казалось бы, безопасной ситуации доверяют свою личную информацию (логин, пароль, ключевое слово и т.д.) злоумышленникам.

Ключевые слова: интернет, личные данные, безопасность, мошенничество, способы кражи, способы предотвращения.

Tuguz N. S., Kazachko A. A.
Kuban state agrarian University named after I. T. Trubilin Krasnodar, Russia

INFORMATION SECURITY AND METHODS OF OBTAINING PERSONAL DATA BY FRAUDSTERS

Annotation: This article discusses methods of identity theft by fraudsters and ways to prevent them. Currently, there is a problem of confidentiality. People carefully hide their personal data and trust them only to trusted services, but insufficiently literate users in the IT sphere may not even suspect that they are in a seemingly secure situation trusting their personal information (username, password, keyword, etc.) to hackers.

Keywords: internet, personal data, security, fraud, theft methods, prevention methods.

Человек 21 века уже не может представить свою жизнь без смартфона. Он стал инструментом для воздействия практически на все сферы жизнедеятельности. Именно простота и удобство привело это устройство к тому, что оно стало необходимостью для каждого. Но не осведомлённый пользователь может даже не догадываться, что скрывается за этой простотой. «Экономическая сфера человеческой деятельности связана с принятием решений в условиях недостатка ин-

формации» [4. С. 139]. «Данную проблему могут решить технологии образования, использующие компьютеры. Таким образом, в программе должны решаться задачи мотивации обучения и компьютеризации» [5. С. 148].

Например, к вам приходит на почту письмо от «официального» представителя вашего мобильного оператора со следующим содержанием: «Специально для вас мы подготовили выгодный тариф, перейдите на сайт и ознакомьтесь с условиями подключения». Вы убеждаетесь в том, что ссылка действительно официального сайта оператора, переходите по ссылке и вам предлагают скачать PDF файл, в котором содержится нужная для вас информация. Вы скачиваете файл, нажимаете на него 2 раза, но он не открывается, нажимаете ещё раз, и снова ничего не происходит. Вы пожимаете плечами и, отвлекаясь уже на другие дела, не предаете значение данному событию, но через несколько дней вы обнаруживаете, что у вас пропали все деньги с банковской карты. Как это могло случиться? Ведь вы не пользовались сомнительными сервисами, нигде не оставляли данные своей карты. Всё произошло именно в тот момент, когда вы нажали на скаченный файл с сайта, который не является официальным. В ссылке на такой сайт латинская буква может быть заменена на русскую, к примеру «о» на «о». Действительно, внешне они полностью идентичны, но находясь в адресной строке являются совершенно разными символами. Таким образом, вы попадаете на сайт злоумышленника и скачиваете файл, при нажатии на который запускается компьютерный вирус [1].

Компьютерный вирус – вид вредоносной программы, написанной злоумышленником, способный создавать копии самого себя, внедряться в код других программ, системную область памяти компьютера, а также в загрузочные секторы. Данная ситуация – отличный пример не нацеленной кибератака. Кибератака – несанкционированное воздействие на вычислительную систему специальными программными средствами с целью нарушения её работы, получения секретной информации и т. п.

Существует два основных типа кибератак:

– целевая кибератака – кибератака, нацеленная на определённого человека, компанию и т.д.

– не нацеленная кибератака – кибератака, не нацеленная на конкретный объект. Осуществляется с помощью рассылок, фишинговых писем и т.п.

Так как не нацеленная кибератака – самая массовая угроза, с которой мы встречаемся каждый день, поэтому поговорим именно о ней. В некоторых случаях даже не обязательно скачивать что-то с интернета, чтобы быть атакованным. Злоумышленники пользуются несовершенством браузеров и других программ на персональных компьютерах, чтобы запустить вирус в случае обычного перехода на сайт по ссылке [2, 3].

В настоящее время хакеры всё чаще обращают своё внимание на мобильные устройства. В них программное обеспечение и приложения проходят огромное количество проверок, что составляет значительные трудности злоумышленникам в поиске каких-либо лазеек, с помощью которых можно совершить кибератаку. Тогда почему же злоумышленники при выборе атакуемых устройств больше отдают предпочтение смартфонам, чем ПК? Ответить на этот вопрос помогут исследования, проведённые великобританскими социологами. В среднем испытуемые люди в молодом возрасте тратили суммарно 5 часов в день, проводя время со смартфоном. При этом они разблокировали телефон более 80 раз за сутки. При этом участники были уверены, что доставали телефон не более 40 раз. По исследованиям «лаборатории Касперского» 40 % людей берут собой в туалет и 20 % принимают с ним ванную. Исходя из этих фактов можно сделать вывод, что человек совершает намного больше каких-либо операций на телефоне, нежели на других устройствах. К тому же, сейчас к многим телефонам современного человека привязаны банковские карты, различные сервисы, пароль от которых у неграмотного пользователя зачастую стоит один и тот же. Такой пользователь становится очень привлекательным для мошенников [6, 7].

В настоящее время уже никто не воспринимает всерьёз сообщения по типу: «Мам, я попал в аварию, отправь на этот номер 5000 рублей». Умнеют пользователи, умнеют и мошенники! Поэтому они придумывают новые способы мошенничества. Приложение «ANCERTRY» - яркий тому пример. Оно якобы помогает найти твоих дальних предков. Для этого нужно ввести дату, место рождения, Ф. И. О нужного вам человека. После этого вам предлагают прислонить палец к месту сканера. Звучит логично, ведь чтобы найти вашего родственника, необходимо скачать вашу биометрию в базу данных и сравнить её с биометрией, к примеру, прадеда. Но многие не задумываются о том, что во времена вашего прадеда никто не собирал биометрию, но люди об этом не задумываются и всё равно подносят палец. После этого пользователи, сами не зная этого, приобретают премиум подписку за 83 фунта. Всё из-за того, что они не прочли пользовательское соглашение. Но читать по 5-6 страниц соглашения зачастую очень утомительно и делают это единицы. В таких ситуациях, как минимум, не стоит давать свои биометрические данные без особой нужды, ведь они так же являются очень важным ключом. То же самое касается и различных согласий на использование встроенных функций и базы данных смартфона (камера, телефонная книга, коренные файлы и т. д). И чем меньше вы будете доверять их сервисам, чем внимательней вы будете читать то, что вам предлагают, тем меньше шанс попасться на уловку мошенников.

Потерять несколько сотен рублей ещё не так страшно, как отдать приложению свои Root права. Пользовательское соглашение приложение так же может не за-

метно вам подсунуть. И вы должны чётко осознавать кому вы их отдаёте. При попадании данных прав в руки злоумышленников, они получают полный доступ к глубинным функциям вашего смартфона: включать камеру в любое время, отслеживать вашу геолокацию, перехватывать все смс, записывать речь диктофона, и пользоваться всем, что позволяет смартфон. Особенно легко атакам поддаются старые устройства, с несовершенной защитой. В этом случае тенденция постоянно менять свой телефон идёт только на пользу вашей личной безопасности, но даже имея самый новый смартфон или компьютер, с самой безупречной защитой, вы не будете застрахованы от попадания в ботнет систему хакера.

Ботнет — компьютерная сеть, состоящая из какого-либо количества хостов с запущенными ботами — автономным программным обеспечением. Бот - специальная программа, выполняющая автоматически и/или по заданному расписанию какие-либо действия через интерфейсы, предназначенные для людей.

Личные данные – не всё, что может понадобиться от вас злоумышленникам. Профессионалы в этом деле могут поставить ваш телефон в армию заражённых устройств. Такие устройства, путём перегрузки, способны вывести из строя целый сайт. Для этого программисту достаточно отдать всего одну команду. Такие устройства зачастую довольно быстро выходят из строя, так как подвергаются большим перегрузкам. Поэтому стоит задуматься, если ваше устройство стало перегреваться или медленнее выполнять.

Библиографический список

1. Кинг Б. Банк 3.0 / Бретт Кинг. – М. ЗАО «Олимп-Бизнесс» 2014

2. Кондратенко Л. Н. Функции многих независимых переменных [Текст] : учеб. пособие / Л. Н. Кондратенко. – Краснодар : ООО «ПринтТерра», 2017. – 95 с.

3. Кондратенко Л. Н., Стариков Л. Ю. Эффективные методы мотивации и стимулирования персонала. В сборнике: РЕГИОНАЛЬНЫЕ ОСОБЕННОСТИ РЫНОЧНЫХ СОЦИАЛЬНО-ЭКОНОМИЧЕСКИХ СИСТЕМ (СТРУКТУР) И ИХ ПРАВОВОЕ ОБЕСПЕЧЕНИЕ. Сборник материалов VII Международной научно-практической конференции. Под редакцией О. С. Кошевого. 2016. С. 238-241.

4. Магсумова Д. М., Николаева Е. Б., Кондратенко Л. Н. Дискретная случайная величина в сфере IT технологий и экономики. В сборнике: Студенческие научные работы землеустроительного факультета. сборник статей по материалам Международной студенческой научно-практической конференции. Ответственный за выпуск И. В. Соколова. 2019. С. 138-142.

5. Тищенко О. Ю., Кондратенко Л. Н. Применение инновационных технологий в процессе обучения математике. // Экономика. Право. Печать. Вестник КСЭИ. 2013. № 4 (60). С. 147-150.

5. ISO/IES 27001-2005 Информационные технологии. Методы обеспечения безопасности – Системы управления информационной безопасностью. 2005

6. Федеральный закон «О персональных данных».27 июля 2006 года № 152-ФЗ. Принят Государственной думой 8 июля 2006 года

7. Исследование журнала “GQ” [Электронный ресурс] Режим доступа: https://nplus1.ru/news/2017/11/10/deep-service